

Masashi TAKUBO, S.N. 10/766,724  
Page 11

Dkt. 2271/71526

REMARKS

The application has been reviewed in light of the Office Action dated July 13, 2007. Claims 1-12, 14, 15, 17, 18 and 20 were pending, with claims 13, 16 and 19 having previously been canceled, without prejudice or disclaimer. By this Amendment, claims 1-10 have been amended to clarify the claimed subject matter. Accordingly, claims 1-12, 14, 15, 17, 18 and 20 are presented for reconsideration, with claims 1-10 being in independent form.

Claim 20 was rejected under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement.

Applicant disagrees. Applicant maintains that adequate written description of the subject matter of claim 20 can be found in the disclosure as originally filed, for example, at page 7, line 21 through page 8, line 2, and page 12, lines 4-11.

Claims 11, 14 and 17 were rejected under 35 U.S.C. §101 as allegedly directed to non-statutory subject matter. The Office Action states that "program storage device readable by the computer system" is functional descriptive material.

However, it is respectfully noted that each of claims 11, 14 and 17 is directed to "machine readable medium embodying a program of instructions executable by the machine" and not to "program storage device readable by the computer system". Accordingly, it is submitted that claims 11, 14 and 17 are directed to statutory subject matter.

Claims 1, 4, 7, 11 and 12 were rejected under 35 U.S.C. § 103(a) as purportedly unpatentable over U.S. Patent No. 7,023,573 to Ohhashi et al. in view of U.S. Patent No. 7,107,395 to Ofek et al. and further in view of U.S. Patent No. 5,958,005 to Thorne et al. Claims 2, 5 and 8 were rejected under 35 U.S.C. 103(a) as purportedly unpatentable over Ohhashi in view of Ofek. Claims 3, 6, and 9 were rejected under 35 U.S.C. 103(a) as purportedly

Masashi TAKUBO, S.N. 10/766,724  
Page 12

Dkt. 2271/71526

unpatentable over Ohhashi in view of Ofek and further in view of Simpson et al. (US 20040036907 A1). Claims 10, 14, 15, 17, and 18 were rejected under 35 U.S.C. 103(a) as purportedly unpatentable over Ohhashi in view of Ofek. Claim 20 was rejected under 35 U.S.C. 103(a) as purportedly unpatentable over Ohhashi in view of Ofek and Thorne and further in view of U.S. Patent No. 6,757,698 to McBride.

Applicant has carefully considered the Examiner's comments and the cited art, and respectfully submits that independent claims 1-10 are patentable over the cited art, for at least the following reasons.

This application relates to an approach devised by applicant for performing a backup function in a facsimile apparatus while maintaining security of confidential communications. Document data received by the facsimile apparatus is stored into a first memory inaccessible through the local area network, and if the received document data is not confidential, the received document data is copied into a second memory accessible through the local area network. Each of independent claims 1-10 addresses these features, as well as additional features.

Ohhashi, as understood by Applicant, proposes an image transmission device which includes a scanning section for scanning a document image and generating image data, a fax sending/receiving section for sending the image data to the external device by the request of the external device, a specific document judging section for judging whether or not the image data generated in the scanning section is that of a specific pre-stored document, and a control section for controlling transmission of the image data by the fax sending/receiving section according to a result of judgment by the specific document judging section, thereby preventing the forgery of a specific document that is enabled by obtaining the image data of such specific documents as

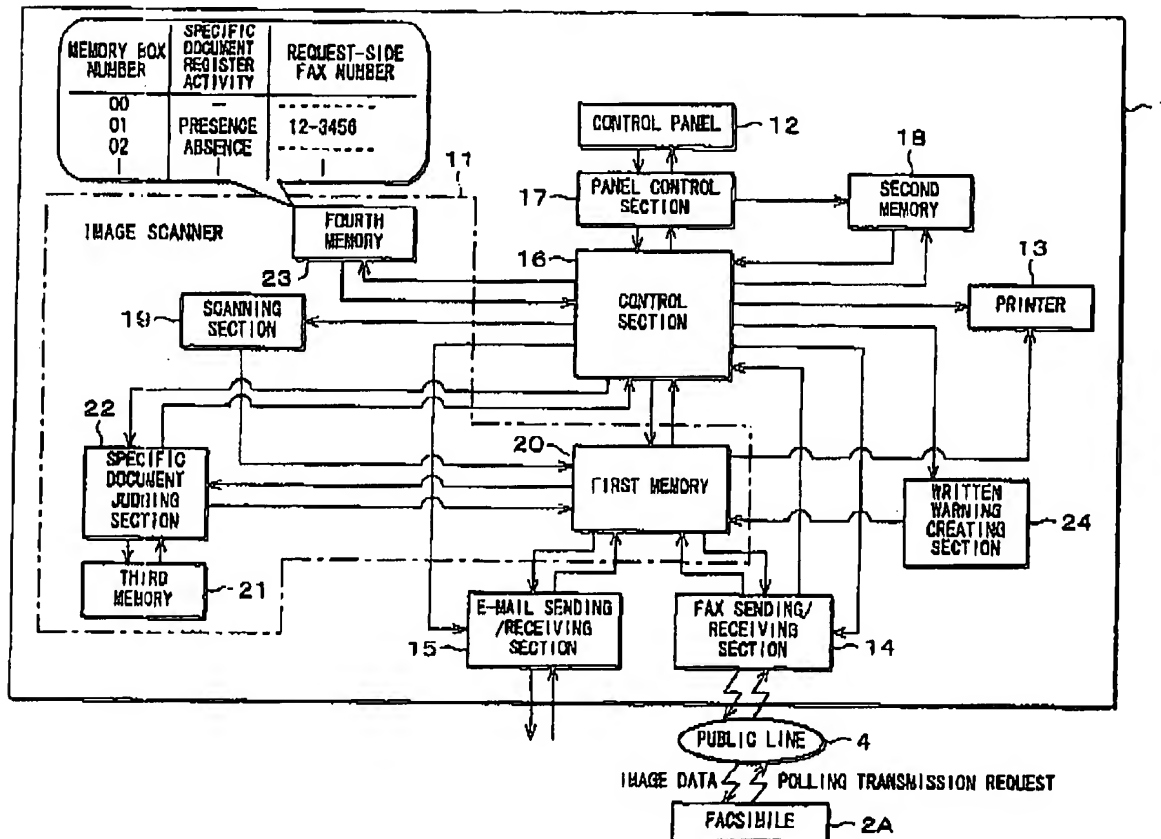
Masashi TAKUBO, S.N. 10/766,724  
Page 13

Dkt. 2271/71526

paper money, valuable securities, etc., scanned by the image transmission device or inputted from the outside to the image transmission device.

The Office Action cites Fig. 7 of Ohhashi, reproduced below:

FIG. 7



The Office Action equates memory 23 in Fig. 7 of Ohhashi with a first storing mechanism, and equates memory 20 in Fig. 7 of Ohhashi with a second storing mechanism.

However, the memory 23 in Fig. 7 of Ohhashi does not store image data. Ohhashi, column 12, lines 27-42, states as follows regarding memory 23:

*Meanwhile, when scanning a document, the fourth memory 23 stores, in each memory box, information of whether or not an activity of registering a specific document ("specific document register activity", hereinafter; forgery) has been executed (information of the "presence or absence of the specific document register*

Masashi TAKUBO, S.N. 10/766,724  
Page 14

Dkt. 2271/71526

*activity") by using each memory box (according to the number attached to each memory box). Further, when a polling transmission request is sent to a memory box indicating the "presence of the a specific document register activity", the fourth memory 23 further stores transmission request sender information, such as the fax number of the facsimile 2A requesting the polling transmission (destination fax number) and the like, and information on the image data registered in the memory box indicating the "presence of the specific document register activity" (specific image information) in each memory box.*

Thus, the memory 23 of Ohhashi is proposed to be used for storing information indicating whether an activity of registering a specific document has been executed, and is not for storing image data.

In addition, Ohhashi does not disclose or suggest that the image transmission device includes a determining mechanism configured to determine whether the received document image data is confidential, as provided by the subject matter of claim 1 of the present application.

Ohhashi is concerned with forgery of "specific documents", such as paper money, valuable securities, etc. (see Field of the Invention and Abstract of Ohhashi). For example, Ohhashi, column 1, lines 14-20, and column 2, line 60 through column 3, line 12, states as follows:

In recent years, a digital color copy machine which has superior color reproducibility and therefore can provide a reproduced image extremely close to its original is manufactured, that is the fruit of years of a technological development. *There is concern, however, that this superior digital color copy machine is likely to be illegally used in the forgery of paper money, valuable securities and the like.*

...  
It is an object of the present invention to provide an image transmission device and an image transmission method which are capable of *preventing an activity of forging a specific document, where either the image data of such a specific document as paper money or valuable securities scanned by an image transmission device or image data of a specific document inputted to the image transmission device from the outside is obtained from an external device.* Further, another object of the present invention is to provide an image transmission device and an image transmission method capable of preventing with an easy configuration the forgery of a specific document with the use of such an image transmission device as a facsimile, and in particular, an image transmission device and an image transmission method

Masashi TAKUBO, S.N. 10/766,724  
Page 15

Dkt. 2271/71526

*capable of preventing, and tracking, the activities of forging an image of a specific document by retrieving the image that is stored in the image transmission device from an external device.*

Ohhashi proposes storing sample data of said specific documents in advance and thereafter judging whether a scanned document is one of said specific documents, by comparing said scanned document with the sample data.

However, the apparatus of Ohhashi does not determine whether the subject document is confidential. It is noted that the specific documents, such as paper money and valuable securities, stored in advance generally are not confidential.

Further, Ohhashi, as acknowledged in the Office Action, does not disclose or suggest that the image transmission device has a backup mechanism. Ohhashi simply is not concerned with backup.

Ofek, as understood by Applicant, proposes a computer system including host computers and storage elements, wherein the host computers are configured into a host domain and the storage elements are configured into a storage domain, the storage domain includes a plurality of primary storage devices and a secondary storage device, and the secondary storage device is coupled to the primary storage devices through a network to provide backup media for the host computers.

However, Ofek, like Ohhashi, is not concerned with whether specific stored image data is confidential. The backup mechanism proposed by Ofek does not make a determination as to whether the stored data is confidential, in the process of making a copy of the stored data for backup.

Thorne, as understood by Applicant, proposes an approach for communicating data text messages, such as e-Mail, between computers connected to a network while providing selectable

Masashi TAKUBO, S.N. 10/766,724  
Page 16

Dkt. 2271/71526

degrees of security for each message. A data message having a header is created in the originating computer which specifies, in addition to the address of the intended recipient computer, one or more security parameters (such as instructions for erasure of the data message following its storage in the recipient computer, instructions as to whether copying, archiving, forwarding and printing of the data message is permitted, etc.) which control the processing of the data message in the recipient computer. The recipient computer processes the data message in accord with the instructions.

The Office Action references Fig. 3 and the archiving function proposed in Thorne.

However, the archiving function proposed in Thorne, Fig. 3, is not contingent on the message being not confidential. Thorne, Fig. 3, clearly proposes that the user can specify whether to archive a message regardless of the level of security set for the message.

Regarding step 542 proposed in Thorne, Thorne proposes that if the user has enabled the archiving feature, a message archive icon is displayed, and the user can thus specify that a specific message is to be archived.

However, Thorne does not disclose or suggest that if an archive command is specified by the user, a determination of whether the message is confidential is made before the message is archived.

Simpson, as understood by Applicant, proposes a system for saving a facsimile message to a personal image repository as a facsimile image in a format compatible with multiple computer operating systems for use with an identity-based imaging system. Each device storing the facsimile message/image is network-accessible. The system proposed by Simpson does not make a determination regarding whether the facsimile message/image includes confidential data or not.

Masashi TAKUBO, S.N. 10/766,724  
Page 17

Dkt. 2271/71526

McBride, as understood by Applicant, proposes an approach for automatically synchronizing data from a host computer to two or more backup data storage locations. One location is on the Internet and a second location is a local data storage location. The apparatus proposed by McBride does not make a determination regarding whether the data to be backed-up includes confidential data or not.

In short, none of the cited references teach or suggest storing received document image data into a first storing mechanism inaccessible through the local area network and a copy of the received document image data into a second storing mechanism accessible through the local area network, determining whether the received document image data is confidential, and canceling storing the copy of the received document image data into the second storing mechanism when the received document image data is determined as confidential, as provided by the subject matter of claim 1 of the present application. Independent claims 4 and 7 are patentably distinct from the cited art for at least similar reasons.

Regarding claims 2, 5 and 8, the apparatus of Ohhashi, as mentioned above, does not determine whether the subject document is confidential, and does not have a backup mechanism, and further the memory 23 of Ohhashi is not for storing document image data. Ofek, as mentioned above, is not concerned with whether specific stored image data is confidential, and the backup mechanism proposed by Ofek does not make a determination as to whether the stored data is confidential, in the process of making a copy of the stored data for backup.

Accordingly, the cited references also fail to teach or suggest a facsimile apparatus comprising a backup arranging mechanism configured to store received document image data into a first storing mechanism inaccessible through the local area network and a copy of the received document image data into a second storing mechanism accessible through the local area

Masashi TAKUBO, S.N. 10/766,724  
Page 18

Dkt. 2271/71526

network, a determining mechanism configured to determine whether the received document image data stored in the second storing mechanism is confidential upon a receipt of a data transmission request for transmitting the received document image data stored in the second storing mechanism from an external terminal through the local area network, and a controlling mechanism configured to refuse the data transmission request from the external terminal through the local area network when the received document image data is determined as confidential by the determining mechanism, as provided by the subject matter of claim 2 of the present application. Independent claims 5 and 8 are patentably distinct from the cited art for at least similar reasons.

Likewise, the cited references fail to teach or suggest a facsimile apparatus comprising a backup arranging mechanism configured to store received document image data into a first storing mechanism inaccessible through the local area network and a copy of the received document image data into a second storing mechanism accessible through the local area network, a determining mechanism configured to determine whether the received document image data stored in the second storing mechanism is confidential upon a receipt of a data transmission request for transmitting the received document image data stored in the second storing mechanism from a web browser through the local area network, and a controlling mechanism configured to refuse the data transmission request from the web browser through the local area network when the received document image data is determined as confidential by the determining mechanism, as provided by the subject matter of claim 3 of the present application. Independent claims 6, 9 and 10 are patentably distinct from the cited art for at least similar reasons.

Accordingly, for at least the above-stated reasons, Applicant respectfully submits that

Masashi TAKUBO, S.N. 10/766,724  
Page 19

Dkt. 2271/71526


independent claims 1-10, and the claims depending therefrom, are patentable over the cited art.

In view of the remarks hereinabove, Applicant submits that the application is now in condition for allowance. Accordingly, Applicant earnestly solicits the allowance of the application.

If a petition for an extension of time is required to make this response timely, this paper should be considered to be such a petition. The Patent Office is hereby authorized to charge any fees that are required in connection with this amendment and to credit any overpayment to our Deposit Account No. 03-3125.

If a telephone interview could advance the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney.

Respectfully submitted,

  
Paul Teng, Reg. No. 40,837  
Attorney for Applicant  
Cooper & Dunham LLP  
Tel.: (212) 278-0400